IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	**v**
v.	:	**CRIMINAL ACTION NO. 19-392**
	:	
MALAN DOUMBIA, *et. al*.	:	

MEMORANDUM OPINION

After a week-long trial, a jury convicted defendants Malan Doumbia and Souleymane Diarra ("Defendants") on all counts of a nine-count indictment which charged them with various fraud, aggravated identity theft, and money laundering offenses. Defendants now move under Federal Rule of Criminal Procedure 29 for a judgment of acquittal. For the reasons that follow, Defendants' motions will be denied.

I. BACKGROUND

As alleged in the indictment, Defendants, along with a fugitive co-conspirator, Souleyman Jallow, carried out a complex credit/debit card fraud scheme from 2012 to 2019. As part of the scheme, Defendants allegedly purchased thousands of stolen credit/debit numbers from darknet websites overseas, and then attempted to withdraw funds from those accounts. In March 2015, following an investigation, United States Secret Service ("USSS") agents executed search warrants at Defendants' residences in Philadelphia. During that search, agents seized the following: card encoding machines; re-encoded cards; blank card stock; and, computers and phones which contained thousands of stolen debit/credit card numbers. Defendants were charged, and ultimately found guilty of: (1) conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; (2) counterfeit access device fraud, in violation of 18 U.S.C. §§ 1029(a)(1) and 2; (3) possession of device-making equipment, in violation of 18 U.S.C. §§1029(a)(4) and 2; (4)

aggravated identity theft, in violation of 18 U.S.C. §§ 1028(a)(1), (c)(5), and 2; and, (4) conspiracy to commit money laundering, in violation of 18 U.S.C. §§ 1956(h), (a)(2)(B)(i) and (a)(2)(A).

During trial, the Government presented the jury with a large swath of evidence. The evidence included, *inter alia*, transcripts of wiretapped conversations between confidential informants and defendants; photos of blank cards and card-making devices found in Defendants' homes; and, the testimony of multiple witnesses involved in the investigation. These witnesses included: (1) Confidential Informant 2 ("CI2"); (2) USSS Special Agent Malaika Crowe; (3) USSS forensic computer agent Bryan Deyoung; and, (4) Department of Homeland Security agent Michael Johnson. The parties also stipulated to a number of facts regarding what certain victims of Defendants' conduct would have testified to regarding their stolen information. Defendant Diarra moves for acquittal on all counts; Defendant Doumbia moves for acquittal only on the conspiracy to commit wire fraud count and the aggravated identity theft counts.

II. STANDARD OF REVIEW

Under Rule 29 of the Federal Rules of Criminal Procedure, a judgment of acquittal must be entered for "any offense for which the evidence is insufficient to sustain a conviction." Fed. R. Crim. P. 29(a). Evidence is insufficient if no "rational trier of fact could have found proof of guilt beyond a reasonable doubt based on the available evidence." *United States v. Caraballo-Rodriguez*, 726 F.3d 418, 430 (3d Cir. 2013) (en banc) (quoting *United States v. Brodie*, 403 F.3d 123, 133 (3d Cir. 2005)). This standard is "highly deferential" to the findings of the jury. *Id.* Review under Rule 29 requires consideration of the entire record—not just pieces of evidence in isolation—in the light most favorable to the prosecution. *Id.* Courts "must be ever vigilant not to usurp the role of the jury by weighing credibility and assigning weight to the evidence." *Id.* (citation omitted) (cleaned up). And to avoid "act[ing] as a thirteenth juror," a

verdict may only be overturned if it "falls below the threshold of bare rationality," *id*. at 431, or "where the prosecution's failure is clear." *United States v. Leon*, 739 F.2d 885, 891 (3d Cir. 1984) (citation omitted). Proving that this standard requires a verdict be overturned is "a very heavy burden." *United States v. Anderson*, 108 F.3d 478, 481 (3d Cir. 1997) (citation omitted).

III. DISCUSSION

A. Count I: Conspiracy to Commit Wire Fraud, 18 U.S.C. § 1349

Both Defendants move for acquittal as to the wire fraud conspiracy count under 18 U.S.C. § 1349 which provides as follows: "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." The statute does not require proof of an overt act. *See United States v. Obaygbona*, 556 F. App'x 161 (3d Cir. 2014). Thus, to establish a violation of 18 U.S.C. § 1349, the Government must have proven the following elements beyond a reasonable doubt: (1) that two or more people agreed to commit wire fraud; (2) that Defendants were members of that agreement; and, (3) that Defendants shared a unity of purpose and the intent to achieve a common goal. *United States v. Rankin*, 870 F.2d 109, 113 (3d Cir. 1989).

A conspiracy can be proven by direct or circumstantial evidence. *Brodie*, 403 F.3d at 134. Its existence can be inferred from evidence of related facts and circumstances "from which it appears, as a reasonable and logical inference, that the activities of the participants could not have been carried on except as a result of a preconceived scheme or common understanding." *Id.* (citation omitted). Inferences drawn, however, cannot be based on "speculation." *United States v. Thomas*, 114 F.3d 403, 406 (3d Cir. 1997); *United States v. Boria*, 592 F.3d 476, 481 (3d Cir. 2010). In reviewing a motion under Rule 29, a court faced with conflicting inferences "must presume—even if it does not affirmatively appear in the record—that the trier of fact

resolved any such conflicts in favor of the prosecution, and must defer to that resolution." *McDaniel v. Brown*, 558 U.S. 120, 133 (2010) (citation and quotation marks omitted).

Diarra and Doumbia first argue that the evidence presented by the Government at trial is insufficient to sustain a conviction because "the Government presented no evidence" to establish that Diarra and Doumbia even know one another, such as a "telephone conversation, [or] text" between the two. However, at trial, the Government established through testimony and other evidence that Defendants went by aliases: Diarra was also known as "Vieux," "V," and "Mike," while Doumbia was known as "Frenchie." The Government then showed that "V" and Doumbia communicated with one another through multiple means. For example, the Government presented photos of Doumbia's phone, which phone displayed multiple messages on WhatsApp from a sender named "V." The messages include numerous credit card numbers from Cathay Bank Taiwan. Doumbia responded with additional numbers and also wrote, "celui-là est bon," which in French means "this one's good." Other exhibits showed that Doumbia and "V" exchanged links to conversations through an app called "Privnote" which sends notes that self-destruct after being sent. And another exchange on August 13, 2018, showed that "V" sent Doumbia a text message of credit card information from China Merchants Bank.

This evidence, taken as a whole, establishes that Diarra and Doumbia knew one another and worked together to share credit card numbers with each other that were not their own. This alone establishes the elements of a conspiracy, *i.e.*, that Defendants knowingly agreed and worked together to achieve the common goal of illegally exchanging credit card numbers.

But even if one were to overlook the above evidence, as Defendants do in their motions, the Government was not legally required to show evidence of direct communication between Diarra and Doumbia. The Government was permitted to present circumstantial evidence of the conspiracy, which it did. For example, CI2 testified at trial that prior to his arrest, he was

involved in the credit card fraud business, and that he knew Diarra through that business. CI2 further testified that Diarra worked with a man named Malan Doumbia, who also went by "Frenchie." CI2 stated that Diarra told him about working with Doumbia, and that "[Diarra] trust[ed] Frenchie," enough to provide Doumbia with fake credit cards which he would use to withdraw cash from banks. The Government also presented transcripts of wiretapped conversations between CI2 and Diarra during which Diarra confirmed that "the French guy's [credit card] numbers really work" and that he knew specific details about how Doumbia conducted his work, including: that Doumbia had a manual device with which to make credit cards; that Doumbia eventually lost that device; and, that when Doumbia received the credit card numbers, "he d[id] not use [them] on the spot. He [waited] for about six month[s] before using them so [the FBI] don't trace them [sic] and know their origin."

Defendants do not address the Government's evidence in their Reply. Instead, they argue that the Government improperly relied on evidence from CI2 to establish the existence of a conspiracy and that "the law does not permit [the finding of] a conspiracy with a Government informant." But the Government's objective at trial was not to show the existence of a conspiracy between CI2 and the Defendants, but rather between Defendants themselves through CI2's testimony and recorded conversations. The Government did present evidence on this theory, and it was rational for the jury to agree with the Government that Defendants were guilty beyond a reasonable doubt of carrying out a conspiracy. Defendants' motions will therefore be denied as to the conspiracy to commit wire fraud count.

B. Count II: Counterfeit Access Device Fraud, 18 U.S.C. § 1029(a)(1) and 2

Diarra next moves for acquittal on the Counterfeit Access Device Fraud Count. 18 U.S.C. § 1029(a)(1). To prove a violation of Section 1029(a)(1), the Government must have proven: (1) that the defendant knowingly and with intent to defraud; (2) produced, trafficked in,

had custody or control of, or possessed; (3) one or more counterfeit access devices. 18 U.S.C. § 1029(a)(1). Section 1029(e)(1) of defines the term "access device" as follows:

> [A]ny card, plate, code, account number electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier , or other means of account access *that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value*, or that can be used to initiate a transfer of funds (other than can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).[1]

18 U.S.C. § 1029(a)(1) (emphasis added). Diarra argues that he is entitled to acquittal on this count because in his view, the Government did not introduce any evidence that the cards found in his possession could "be used . . . to obtain money, goods, services, or any other thing of value," *i.e.,* were actually functional when found. Diarra cites to *United States v. Onyesoh*, 674 F.3d 1157 (9th Cir. 2012) for his understanding of this "usability" requirement. There, the Court concluded that a reading of the statute required the Government to show that the cards at issue could at that moment be used to obtain money. *Id.* at 1160.

In response, the Government notes that all other circuits which have considered the meaning of "access device" have rejected the Ninth Circuit's reading of the term. *See, e.g., United States v. Carver,* 916 F.3d 398, 402 (4th Cir. 2019); *United States v. Moon*, 808 F.3d 1085, 1092 (6th Cir. 2015) (rejecting *Onyesoh* "usability" requirement); *United States v. Moore*, 788 F.3d 693, 695 (7th Cir. 2015); *United States v. Cardenas*, 598 F. App'x 264, 267 (5th Cir. 2015); *United States v. Bermudez*, 536 Fed. App'x 869, 871 (11th Cir. 2013); *United States v. Heath*, 424 F. App'x 730, 736-37 (10th Cir. 2011); *United States v. Volynskiy*, 431 F. App'x 8, 9-10 (2d Cir. 2011). In rejecting *Onyesoh*, these courts often turn to the statute's definition of

[1] A "counterfeit access device," in turn, means "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device." 18 U.S.C. § 1029(e)(2).

the term "unauthorized access device." That term is defined as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." 18 U.S.C. § 1029(e)(3). The courts then note that if "access device" were only to encompass "usable" devices, it would render the term "unauthorized access device" under 1029(a)(3) an oxymoron because it would refer to any "functional" device "that is *expired, revoked, canceled*, or obtained with intent to defraud." *See, e.g., Carver*, 916 F.3d at 402-03 ("Expired, revoked, or canceled cards cannot be used to obtain money, and so *Onyesoh* would have three words in its statutory definition that mean nothing.")

While the Third Circuit has yet to issue a precedential opinion discussing the "usability" requirement in Section 1029, in an unpublished opinion, it discussed the definition of "access device fraud" in the context of a defendant who raised a similar "usability" argument after he was sentenced. *United States v. Jones*, 332 F. App'x 801, 807 (3d Cir. 2009). There, the Court of Appeals stated that "the Government was not required to present evidence from banks and other financial institutions that the account numbers . . . *could actually be used* to acquire things of value. The Government simply had to show that the account numbers *were capable* of obtaining things of value." *Id*. (emphasis added). It noted that in the case before it, the "account numbers had the requisite indicia of being capable of use to obtain things of value because they had either been used for that purpose (as evidenced by the receipts and Comcast records) or had been extracted from the magnetic strip on credit cards by skimmers." *Id*.

This Court finds the rationale in the Third Circuit's unpublished opinion persuasive. Here too, the Government presented "the requisite indicia" of the numbers being capable of use to obtain things of value. For example, the Government showed a transcript of a wiretapped conversation between CI2 and Diarra in which CI2 asked Diarra whether to use the card numbers Diarra gave him at Walmart or Target. Diarra responded, "It works in either." Similarly, in

another conversation between Diarra and CI2, Diarra confirms that the fake cards he gave CI2 were functional, saying "you could insert the card [in an ATM] and withdraw as much as you want." Moreover, Agent Crowe testified that after setting up a meeting between CI2 and Diarra during which Diarra gave CI2 various cards, she was able to inspect those cards to find that the magnetic strip numbers were altered to match the numbers on the front of the cards, thereby making them functional for use. Agent Crowe also testified that she found cards containing victim information in the magnetic strips in Diarra's home, suggesting that such cards would be usable. A rational jury, viewing the above evidence as a whole, may have thus reasonably concluded that Diarra was in possession of counterfeit "access devices" within the meaning of the statute.[2]

Diarra also moves for acquittal on the aiding and abetting count under 18 U.S.C. § 2. To prove guilt under this charge, the Government must have shown: (1) that another defendant committed a substantive offense; and (2) the one charged with aiding and abetting knew of the commission of the substantive offense and acted to facilitate it. *United States v. Mercado*, 610 F.3d 841, 846 (3d Cir. 2010). Diarra argues that "no [] evidence" in support of an aiding and abetting theory "exists in this case." However, at trial, the Government presented evidence that met each element of the aiding and abetting statute as to Diarra. First, the jury found—and Doumbia does not dispute—guilt of a substantive offense, which here is counterfeit access device fraud. Second, the Government showed that Diarra knew that Doumbia was committing counterfeit access device fraud. As explained *supra,* Diarra was caught on tape multiple times referring to Doumbia's operations, including his strategic use of credit card numbers to avoid

[2] Because the Government presented sufficient evidence that Diarra possessed "access devices," within the meaning of Section 1029, the Court need not reach Diarra's argument concerning whether he can be found guilty by way of "constructive possession" of any devices by Defendants Doumbia or Jallow.

detection from the FBI and the fact that Doumbia's numbers actually worked. Finally, Diarra acted to facilitate Doumbia's fraud by, *inter alia*, sending him a message containing credit card information to Doumbia on August 13, 2018. A reasonable jury could thus find that Diarra aided and abetted the commission of Doumbia's counterfeit access device fraud.

C. Count III: Possession of Device-Making Equipment, 18 U.S.C. § 1029(a)(4) and 2

Diarra also moves for acquittal on Count III, which is for possession of device making equipment. To prove a violation of 18 U.S.C. § 1029(a)(4), the Government must have shown: (1) that the defendant knowingly and with intent to defraud; (2) "produc[ed], traffic[ked] in, ha[d] custody or control of, or possess[ed]; (3) device making equipment. 18 U.S.C. § 1029(a)(4). "Device making equipment" means "any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device." 18 U.S.C. § 1029(e)(6).

Diarra contends that the Government failed to prove his possession of device-making equipment because no card re-encoders or embossers were found in his own apartment, as opposed to in Jallow's and Doumbia's apartments. In response, the Government argues that it was not limited—under the terms of the statute—to showing that Diarra "possessed" this equipment in his home, but that it could also show that Diarra "had custody or control of" such equipment, which it reads to encompass as having "control over device-making equipment that was in someone else's hands." *See* L. Sand, *et al*, Modern Federal Jury Instructions – Criminal, Instruction 40-8 (2015). Diarra argues that the Government did not introduce sufficient evidence to support a finding of guilt on this theory.

But at trial, the Government showed that Diarra gave CI2 numerous counterfeit cards with CI2's names printed on them. The Government also showed that Diarra knew that Jallow had a re-encoding machine, and that Doumbia had an embossing machine, and worked with both

individuals previously. The Government presented sufficient evidence from which a reasonable jury could infer that Diarra could not have made the cards without "custody or control" over the equipment of his co-conspirators.[3]

Diarra also argues that he cannot be found guilty of aiding and abetting "for the reasons set forth in Section B" of his brief, *i.e.,* the section discussing the Government's alleged failure to provide the jury with evidence of his aiding and abetting Counterfeit Access Device Fraud. But at trial, the Government did in fact provide the jury with evidence from which it could reasonably conclude that Diarra was guilty of this charge. First, the jury found—and Doumbia does not dispute—guilt of a substantive offense, which here is possession of device-making equipment. Second, the Government showed that Diarra knew that Doumbia possessed device-making equipment: he explained to CI2 during a recorded conversation that Doumbia had a "small device" to make cards with as well as fake credit cards made from stolen numbers. Finally, Diarra acted to facilitate Doumbia's acts by, *inter alia*, sending him a message containing credit card information on August 13, 2018. A reasonable jury could thus find that Diarra aided and abetted the commission of Doumbia's possession of device-making equipment.

D. Counts IV-VIII: Aggravated Identity Fraud, 18 U.S.C. §§1028(a)(1), (c)(5) and 2

Diarra and Doumbia both move for acquittal with respect to the five aggravated identity theft counts. To prove a violation of 18 U.S.C. § 1028A, the Government must have shown that:

[3] Setting aside the meaning of "custody or control," Diarra's challenge would also fail under the *Pinkerton* theory pursued by the Government. The Government had alleged that Diarra was a conspirator and thus responsible for any reasonably foreseeable crimes committed by his co-conspirators as long as they were committed during and in furtherance of the conspiracy. *United States v. Ramos*, 147 F.3d 281, 286 (3d Cir. 1998). At a minimum, the evidence clearly shows that Jallow and Doumbia possessed the device-making equipment during the term of the conspiracy, and that that their possession of the same was reasonably foreseeable and done in furtherance of the conspiracy. Thus, Diarra bears responsibility as to this Count as a co-conspirator. *See, e.g., United States v. Herrington*, 719 F. App'x 106, 111 (3d Cir. 2017).

(1) during and in relation to a bank fraud or access device fraud; (2) the defendant transferred, possessed, or used; (3) a means of identification of another person; (4) the defendant acted without legal authority; and, (5) the defendant acted knowingly. 18 U.S.C. § 1028A.

Diarra advances numerous arguments regarding this count, while Doumbia advances one. First, both Defendants argue that the Government did not show that they knew the information "belonged to real people." In support of this argument, Defendants cite the Supreme Court's opinion in *Flores-Figueroa v. United States*, 556 U.S. 646 (2009). There, the Court held that the aggravated identity theft statute requires proof the defendant knew the means of identification actually belonged to another person. *Id.* at 646. The Court recognized, however, that "in the classic case of identity theft, intent is generally not difficult to prove." *Id.* at 656. For example, "where a defendant has used another person's identification information to get access to that person's bank account, the Government can prove knowledge with little difficulty." *Id.* Under *Flores-Figueroa*, therefore, the Government's burden of proving knowledge in a case involving fraud "is minimal." *United States v. Norman*, 465 F. App'x 110, 119 (3d Cir. 2012).

In a number of unpublished opinions, the Third Circuit has found that proof of knowledge in identity theft cases may hinge on circumstantial evidence and inferences. For example, in *Herrington*, 719 F. App'x at 110, the Court found that a jury could rely on the inference that "anyone would know that a bank loan would only be granted to a real person with a real social security number." Similarly, the Third Circuit found that a jury could credit the testimony of a former associate in the fraud scheme that "the scam would not work unless the victims were real." *Id.; see also, Norman*, 465 F. App'x at 118-19 ("Because Smith's involvement in the bank fraud scheme would have been pointless if the means of identification did not belong to real customers, the Government's burden was met.")

Here, the Government presented extensive evidence that Defendants wired money and

bitcoin abroad to obtain personal identifying information over the dark web, including dates of birth, social security numbers, credit card numbers, telephone numbers, and employment information. The Government also showed evidence—in the form of wiretapped conversations between CI2 and Diarra, for example—that Defendants were making substantial amounts of money through use of this personal information. *See, e.g.*, Ex. 11 ("this money is better than the mafia"). A jury could reasonably infer that Defendants knew that the information they paid for belonged to real people because Defendants would not have—over the course of seven years—paid for or profited from information that belonged to no one. *See, e.g., United States v. Casellas*, 842 F. App'x 95, 97 (9th Cir. 2021) (finding that a rational juror could have inferred the defendant knew that the victim information was real when the defendant possessed the victim's social security number, address, birthdate, and employment information). The Government thus met its "minimal" burden to established Defendants' knowledge on these counts.

Second, Diarra argues that because Counts Fix, Six and Eight involved Reliance Bank, which is located in Pennsylvania, "there is [] no evidence in this record that" the transactions at issue "affected interstate commerce." This argument is easily disposed of. Reliance Bank engages in interstate commerce, and as shown as trial, some of the stolen credit/debit card transactions occurred out of state. For example, certain transactions occurred in California. The Government therefore showed a sufficient next with interstate commerce. *See, e.g., United States v. Klopf*, 423 F.3d 1228, 1240 (11th Cir. 2005) ("[C]redit cards generally are issued to applicants by out-of-state financial institutions, and credit-card account numbers travel across state lines, both electronically and by mail. By making purchases and withdrawals with the fraudulently obtained credit cards, Klopf engaged in interstate financial transactions.")

Third, Diarra argues that the Government did not present the jury with sufficient evidence

that he actually used the stolen credit card information. But the Government was not limited to showing actual use of the numbers. Rather, violation of the law includes "knowingly *transfer[ring], possess[ing],* or us[ing], without lawful authority, a means of identification of another person" "during and in relation to" access device fraud. 18 U.S.C. § 1028A (emphasis added). As discussed *supra*, the Government showed evidence of Diarra's possession of personally identifying information, such as victims' social security numbers, credit card numbers, and dates of birth, which he sent by electronic messages to Doumbia. The Government also showed that Diarra had 17 stolen credit card numbers on the computer found in his home. It thus presented evidence at trial from which a jury could reasonably conclude that Diarra was guilty of Section 1208A.[4]

E. Count IX- Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(a)(2)(B)(i)

Finally, Diarra moves for acquittal on the conspiracy to commit international money laundering count, which required the Government to prove beyond a reasonable doubt a: (1) conspiracy to commit money laundering under 18 U.S.C. § 1956(h); and, (2) international money laundering under 18 U.S.C. § 1956(a)(2)(B)(i). Diarra's challenge only concerns the latter.

To obtain a conviction under 18 U.S.C. § 1956(a)(2)(B)(i), the Government was required to prove that Diarra (1) attempted to transfer funds from the United States to a place abroad, (2) knew that those funds represented the proceeds of some form of unlawful activity, and (3) knew that such transfer was designed to conceal or disguise the nature, location, source, ownership, or

[4] Diarra also argues that "there is no evidence that these [stolen] numbers were in the exclusive possession of defendants Doumbia and Jallow. Bulk numbers purchased on the dark web are likely sold to many criminals and there was no testimony in the record as to exclusivity." But Diarra does not explain or cite to any case law explaining why "exclusive possession" of such information is relevant to sustaining a verdict as to aggravated identity fraud.

control of the funds. *Regalado Cuellar v. United States*, 553 U.S. 550, 561 (2008). According to Diarra, all the Government presented as to the third element is "scant evidence of a few wire transfers in small denominations to Ghana and Russia." In his view, "the wiring of money to an overseas account, without more, cannot support a finding that [he] was acting to conceal the nature, location, source, ownership or control of the money."

Under Section 1956, evidence of a purpose to conceal can come in many forms, including "statements by a defendant probative of intent to conceal; unusual secrecy surrounding the transaction; structuring the transaction in a way to avoid attention . . . [and] using third parties to conceal the real owner." *United States v. Garcia-Emanuel*, 14 F.3d 1469, 1475-76 (10th Cir. 1994) (citing cases, including *United States v. Massac*, 867 F.2d 174, 178 (3d Cir. 1989)).

Contrary to Diarra's assertions, the Government did not merely present "scant evidence" of international wires at trial to support its theory of intended concealment. Aside from the wire transfers referred to above, Agent Crowe testified—referring to notes she had taken during her search of Diarra's phone—that Diarra instructed his girlfriend to send wires to individuals in Ukraine and Russia to obtain fraudulent credit card numbers. The jury was able to review Agent Crowe's notes, which contained details about the messages "Mike," *i.e.*, Diarra, would send to his girlfriend regarding who should be marked as the senders and receivers of the wires. Taken together, this evidence demonstrated Diarra's intent to conceal funds, by, *inter alia*: (1) using the alias "Mike," instead of his real name when providing his girlfriend with instructions on how to wire the funds; (2) telling her to use different names for the designated sender of the wires instead of his own; and, (3) having her send the wires instead of himself. The evidence was sufficient to permit a reasonable jury to find that Diarra knew that the wire transactions were designed to conceal the nature of the funds. *See, e.g., United States v. Omoruyi*, 260 F.3d 291, 295-96 (3d Cir. 2001) (holding that evidence established defendant's intent to conceal nature of

proceeds under Section 1956 where he deposited money in bank accounts under false names and used false identification to withdraw it). Diarra's motion for acquittal on this Count will therefore be denied.[5]

An appropriate order follows.

BY THE COURT:

/s/ Wendy Beetlestone

WENDY BEETLESTONE, J.

[5] Diarra also contends that the Government did not present sufficient evidence for a conviction under Section 1956 (a)(2)(B)(i) in that the evidence did not prove any "connection between any stolen card numbers and the wire transfers," *i.e.*, that the wires were sent for an illegal purpose. But showing transfer of funds for an illegal purpose is not an element of Section (2)(B)(i). As explained *supra*, the elements of a Section (2)(B)(i) violation are: (1) transfer of funds from the United States to a place abroad, (2) knowledge that those funds represented the proceeds of some form of unlawful activity, and (3) knowledge that such transfer was designed to conceal or disguise the nature of the funds. *Cuellar*, 553 U.S. at 561.

At best, Diarra seems to be arguing that the Government did not meet an element of the other Section of the money laundering statute he was convicted of, Section 1956(a)(2)(A). That provision forbids transfers of money to places outside of the United States "with the intent to promote the carrying on of specified unlawful activity." 18 U.S.C. 1956(a)(2)(A). But even construing Diarra's argument favorably to fit under the correct legal framework, Diarra still fails to meet his "heavy burden" on his motion. At trial, the Government did in fact demonstrate a "connection" between Diarra's wires and the fraudulent credit card numbers he obtained, *i.e.*, that he had the requisite "intent to promote the carrying on of specified unlawful activity." For example, CI2 testified that based on his experience working with Diarra, he knew that Diarra sent wire transfers using Western Union to places like Russia and Ukraine so that Diarra could obtain credit card numbers. Further, Agent Crowe's notes and testimony showed that Diarra instructed his girlfriend to search the web for "dumps" to buy. Agent Crowe explained that "dumps" refer to fraudulently obtained credit card numbers. *Id*. Agent Crowe's notes also showed that Diarra's phone contained an image of a website where he could buy 14 credit card numbers for a cost of $917. A rational jury could thus infer that money was sent "with the intent to promote the carrying on of specified unlawful activity." 18 U.S.C. 1956(a)(2)(A).